UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/552,878	04/20/2000	John D. Abromavage	55789.000003	5009

7590 01/30/2004

Brett C. Martin
1650 Tysons Blvd.
McLean, VA 22102

EXAMINER
EL CHANTI, HUSSEIN A

ART UNIT	PAPER NUMBER
2157	10

DATE MAILED: 01/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/552,878	ABROMAVAGE ET AL.	
	Examiner	Art Unit	
	Hussein A El-chanti	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 April 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 April 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *3,4,8* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. This action is responsive to application filed on Apr. 20, 2000. Claims 1-54 are pending examination.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: Line 17 of page 8 includes reference No. "114" which is not found in the drawings.. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: reference "160" is not found in the specification. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

4. Applicant has submitted formal drawings that were received on May 21, 2002. The formal drawings clearly do not belong to application 09/552,878. The formal drawings belong to an application titled "Plastic Heat Exchanger And Core Thereof". The examiner did not consider the formal drawings submitted by the applicant. New formal drawings are required to be submitted by the applicant.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by

another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-15 and 20-28 are rejected under 35 U.S.C. 102(e) as being anticipated by Riddle et al., U.S. Patent No. 6,457,051 (referred to hereafter as Riddle).

As to claim 1, Riddle teaches a system for extracting information from network data, comprising:

an input interface connected to at least one source of network data (see col. 7 lines 3-17 and 45-64); and

a network event sensor, communicating with the input interface, the network event sensor applying at least a lexical engine to the network data to identify at least one network event (see col. 13 lines 57-col. 14 lines 8).

As to claim 2, Riddle teaches the system of claim 1, wherein the at least one source of network data comprises an observation port connected to a network and continuously capturing network data from the network (see col. 13 lines 57-col. 14 lines 8).

As to claim 3, Riddle teaches the system of claim 2, wherein the observation port comprises a network interface card (see col. 7 lines 3-17).

As to claim 4, Riddle teaches the system of claim 3, wherein the network comprises at least one of an Ethernet network, a token ring network, and a TCP/IP network (see col. 7 lines 3-17).

As to claim 5, Riddle teaches the system of claim 3, wherein the network interface card is invisible to the network (see col. 7 lines 3-17).

As to claim 6, Riddle teaches the system of claim 1, wherein the at least one source of network data comprises stored network data (see col. 7 lines 35-44).

As to claim 7, Riddle teaches the system of claim 6, wherein the stored network data comprise at least one of captured network files, Website mirrors, archives of Usenet files, and archives of email files (see col. 7 lines 35-44).

As to claim 8, Riddle teaches the system of claim 1, further comprising an interpreter module, the interpreter module scanning the network data to generate logical groupings of the network data (see col. 13 lines 42-col. 14 lines 8).

As to claim 9, Riddle teaches the system of claim 8, wherein the logical groupings comprise packets (see col. 4 lines 7-17).

As to claim 10, Riddle teaches the system of claim 8, wherein the interpreter module removes low level encoding information from the network data to generate the logical groupings (see col. 13 lines 42-col. 14 lines 8).

As to claim 11, Riddle teaches the system of claim 10 wherein the low-level encoding information removed by the interpreter module comprises hardware addressing information (see col. 13 lines 42-col. 14 lines 8).

As to claim 12, Riddle teaches the system of claim 8, further comprising an assembler module, communicating with the interpreter module, the assembler module scanning the logical groupings to generate at least one session object (see col. 13 lines 42-col. 14 lines 8 and Fig. 3).

As to claim 13, Riddle teaches the system of claim 12, wherein the at least one session object comprises at least one session file (see col. 13 lines 41-55).

As to claim 14, Riddle teaches the system of claim 12, wherein the assembler module scans the logical groupings by examining at least one of source address, destination address, sequence numbers, source port, and destination port to generate the at least one session object (see col. 13 lines 42-col. 14 lines 8).

As to claim 15, Riddle teaches the system of claim 12, wherein the network event sensor applies the lexical engine to the at least one session object to identify the at least one network event as at least one of a predetermined set of event types (see col. 13 lines 42-col. 14 lines 8).

As to claim 20, Riddle teaches the system of claim 12, wherein the network event sensor applies the lexical engine recursively to identify more than one event type contained in the at least one session object (see col. 13 lines 55-col. 14 lines 3).

As to claim 21, Riddle teaches the system of claim 15, further comprising an extractor module, the extractor module extracting the at least one network event from the at least one session object according to the at least one of a predetermined set of event types (see col. 13 lines 42-col. 14 lines 8).

As to claim 22, Riddle teaches the system of claim 21, wherein the extractor module comprises a library of extractor types, each of the extractor types corresponding to at least one of the at least one of a predetermined set of event types (see col. 13 lines 42-col. 14 lines 8).

As to claim 23, Riddle teaches the system of claim 22, wherein the extractor module stores a minimum subset of the network data to reconstruct the at least one network event (see col. 7 lines 35-44).

As to claim 24, Riddle teaches the system of claim 23, wherein the minimum subset of the network data is stored in a database (see col. 13 lines 41-55).

As to claim 25, Riddle teaches the system of claim 24, further comprising a presentation module, communicating with the database, the presentation module querying the database for information related to the at least one network event (see col. 13 lines 41-55).

As to claim 26, Riddle teaches the system of claim 1, wherein the network event sensor also applies a port detection engine to the network data to identify the at least one network event (see col. 13 lines 55-col. 14 lines 2)).

As to claim 27, Riddle teaches the system of claim 1, wherein the at least one source of network data comprises a plurality of sources of network data (see col. 9 lines 55-col. 10 lines 9).

As to claim 28, Riddle teaches a method for extracting information from network data, comprising the steps of:

a) receiving network data from at least one source of network data (see col. 7 lines 3-17 and 45-64); and

b) applying at least a lexical engine to the network data to identify at least one network event (see col. 13 lines 57-col. 14 lines 8).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 16-19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Riddle in view of Tang, U.S. Patent No. 6,378,126.

As to claim 16, Riddle teaches the network event sensor applies the lexical engine to the at least one session object to identify the at least one network event as at least one of a predetermined set of event types (see the rejection of claim 15).

Riddle does not explicitly teach the claimed limitation "lexical engine detects the presence of at least one predefined keyword to identify the at least one of a predetermined set of event types". However Tang teaches a lexical scanner that identifies keywords (see col. 4 lines 17-28).

It would have been obvious for one of the ordinary skill in the art at the time of the invention to modify Riddle by incorporating the step of identifying keywords as taught by Tang because doing so would allow the user to classify traffic into more details by inputting user specified keywords.

As to claim 17, Riddle teaches the system of claim 16, wherein the predetermined set of event types 5 comprises at least one of TCP, IP, UDP, SMTP, HTTP, NNTP, FTP, TELNET, DNS, RIP, BGP, MAIL, NEWS, HTML, XML, PGP, S/NIZME, POP, MAP, V-CARD, ICMP, NetBUI, IPX and SPX (see col. 7 lines 45-5).

As to claim 18, Riddle teaches the system of claim 16, wherein the lexical engine accumulates a total number of occurrences for the at least one predefined keyword to identify the event type (see col. 13 lines 50-56).

As to claim 19, Riddle teaches the system of claim 18, wherein the lexical engine applies a threshold to the number of occurrences to identify the event type (see col. 14 lines 1-8).

7. Claims 29-54 do not add or define any additional limitation over claims 1-28 and therefore are rejected for similar reasons.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Intelligent Network Interface System And Method For Protocol Processing by Boucher et al., U.S. Patent No. 6,226,680.
- System To Transition An Enterprise To A Distributed Infrastructure by Eager et al., U.S. Patent No. 5,960,200.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hussein A El-chanti whose telephone number is (703)305-4652. The examiner can normally be reached on Mon-Fri 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (703)308-7562. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-3900.

Hussein El-chanti

Jan. 20, 2004

ARIO ETIENNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100